PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F

A2

(11) International Publication Number: WO 97/16782

(43) International Publication Date: 9 May 1997 (09.05.97)

(21) International Application Number: PCT/GB96/02561

(22) International Filing Date: 17 October 1996 (17.10.96)

(30) Priority Data:

9521407.8	18 October 1995 (18.10.95)	GB
9602615.8	9 February 1996 (09.02.96)	GB

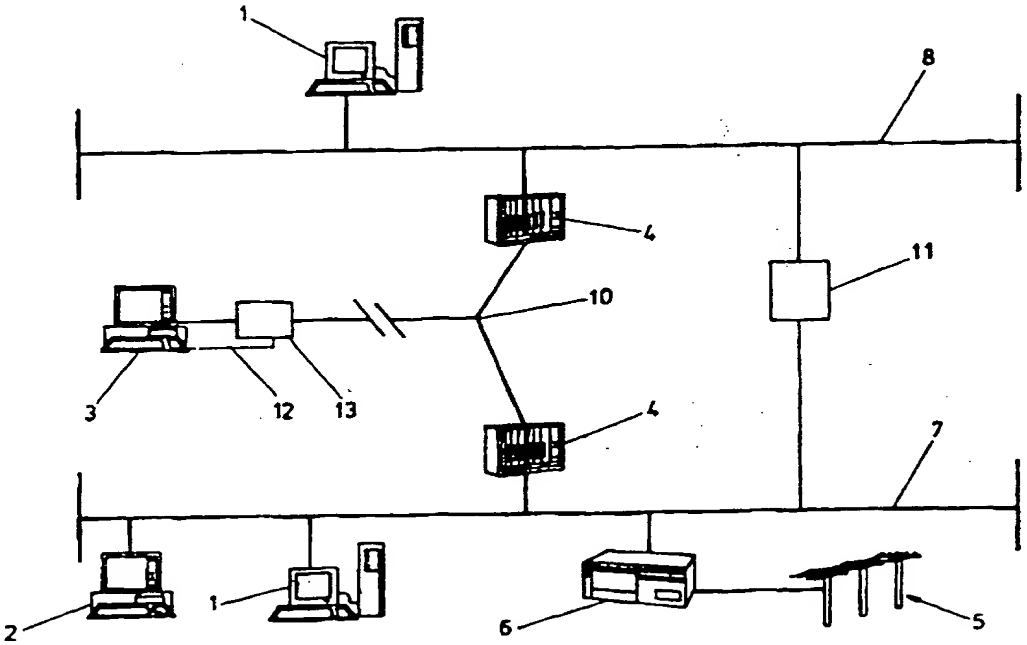
(71)(72) Applicant and Inventor: HOLBOROW, Leslie, Christopher [GB/GB]; 10 Mydam Lane, Gorseinon, Nr. Swansea, West Glamorgan SA4 4YA (GB).

(74) Agent: GIBSON, Stewart, Harry; Urquhart-Dykes & Lord, Three Trinity Court, 21-27 Newport Road, Cardiff CF2 1AA (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: COMPUTER NETWORK SECURITY ARRANGEMENTS



(57) Abstract

A computer system comprises two or more independent data networks (7, 8) and at least one computer terminal (3). The or each computer terminal has a switching means (13) associated with it, for selectively interfacing that terminal with any one of the data networks, one-at-a-time, via respective communication channels.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

Computer Network Security Arrangements

The present invention relates to computer network security, and more particularly to arrangements for providing security to or between a plurality of computer data networks.

An increasingly important concern for computer system developers is that of data security. Where a computer system comprises more than one data network, or provides a link to some remote data network, then the potential exists for unauthorised access to or transfer of confidential information between those networks via the physical interfaces which are provided between them.

The conventional approach to securing a network interface is to provide a so-called 'fire-wall'. Such a device provides security by filtering the data traffic between two or more networks according to pre-defined software instructions. A 'fire-wall' arrangement is, however, costly to install and maintain, remains susceptible to 'hacking', and is not resilient to the failure of its interface circuitry.

I have now devised arrangements which overcome the above-mentioned limitations associated with existing network security.

In accordance with the present invention, there is provided a computer system which comprises two or more independent data networks and at least one computer terminal, the or each computer terminal having a switching means associated therewith for selectively interfacing that computer terminal with any one of said data networks, one-at-a-time, via respective communication channels.

In this system, each computer terminal interfaces with the networks one-at-a-time, and therefore never with two (or more) networks simultaneously. Accordingly, there is never a direct communication channel or link established between different networks.

It is however possible to provide a link, such as an electronic mail (e-mail) link, between two networks, providing such a link does not provide direct access, from one network, to any data storage or processing equipment on the other network.

In the above-defined computer system, one of the networks may be an external network, e.g. the Internet. Two or more of the networks may be provided in a common organisation, in which it is required to restrict the access between those networks.

The switching means may be incorporated in the respective computer terminal or it may form a separate unit connected to that computer terminal. Typically each computer terminal comprises a personal computer (PC).

Preferably the switching means comprises a plurality of data routing circuits which are electrically or electronically re-configurable according to control signals issued by the respective computer terminal.

Preferably the electronically re-configurable data routing circuits comprise electromagnetic relay devices driven by Darlington amplifier circuits.

Preferably the switching means receives data and/or control signals either directly via the internal bus system of the respective computer terminal, or indirectly via a parallel or serial interface card.

Preferably the switching means is controlled via software driver routines running on the respective computer terminal.

Preferably the computer network data is carried by an 'unshielded twisted pair' cable but may instead be carried by other cable types such as shielded coaxial or fibre-optic.

Preferably the switching means routes data via one or other of two 4-way data channels comprising an 8-way 'splitter' cable.

Also in accordance with the present invention, there is provided a computer input/output interface card, comprising parallel and/or serial interface circuitry, and switching means for selectively interfacing said interface circuitry with any one of a plurality of independent computer data networks, one-at-a-time, vie respective communication channels.

Further in accordance with the present invention, there is provided a switching device for selectively interfacing a computer with any one of a plurality of independent data networks, one-at-a-time, via respective communication channels.

An embodiment of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which:

FIGURE 1 is a schematic diagram of a prior art computer system;

FIGURE 2 is a schematic diagram of a computer system in accordance with the present invention;

FIGURE 3 is a circuit diagram of an electronic switching device in accordance with the present invention; and

FIGURE 4 is a schematic showing two possible data channel assignments which can be provided by the device of Figure 3.

Referring to Figure 1 of the drawings, there is shown a typical prior art computer system comprising first and second computer data networks 7,8 each supporting a variety of hardware elements such as file servers 1 and computer terminals 2. The two networks are interconnected by a common data channel via respective interface circuitry or 'hubs' 4. The second network 7 is additionally connected to a remote site via a telephone system 5.

A 'fire-wall' or programmable network access device 9 is provided between the two networks and another such device 6 is provided between the second network and the telephone system. These devices are intended to provide network security by filtering the data passing between respective networks, permitting data access and transfer only in accordance with pre-defined access tables, passwords etc.

Such a 'fire-wall' network interface has a number of significant disadvantages. Firstly, it is costly to install and maintain, often requiring a systems engineer to supervise its operation. Secondly, by sustaining a permanent hardware link between the two networks, such an interface is inherently susceptible to software 'hacking' or to malicious infection with a computer virus. Thirdly, as only a single data channel is provided between the two networks, the failure or incorrect functioning of the intermediate 'fire-wall' device will critically affect all communications between the two networks.

Figure 2 illustrates a computer system in accordance with the present invention, wherein the need for a 'fire-wall' device between the two data networks has be obviated. Each computer terminal e.g. 3 is provided with a re-configurable electronic switching device 13 that allows it to be connected to one or other of the data networks 7,8 according to a control signal 12 from the respective computer terminal 3. A splitter cable connects the appropriate cable cores from the computer terminal 3 to its respective interface hub 10.

Such an arrangement has the important advantage that no direct communications channel or link ever exists between the two networks, which might allow direct access to one network from the other. For example, in Figure 2, whilst computer terminal 3 may access either network 7 or network 8, network 8 is secure from any attempted access via a terminal not provided with an electronic switching device 13, or from a remote site connected to network 7 via the telephone system 5 and 'fire-wall' 6.

A further point to note is that in a system comprising a number of computer terminals, wherein each terminal is connected via a network switching device 13, that connection is fully independent of all others. Therefore, in the event that the network switching device associated with any one terminal should fail, full network access is still available to all other terminals

It is however possible for the system to include a link between the two networks, providing this does not give direct access, from one network, to any data storage or processing equipment on the other network. Thus, an electronic mail (e-mail) link 11 may be provided between the networks.

The switching between the networks is controlled by the respective computer terminal: this can be achieved through use of any suitable operating system run on that terminal (e.g. Windows).

Figure 3 is a schematic diagram of an electronic circuit suitable for implementing the electronic switching device 13 and comprises a 4-way data input 20 from a computer 'PC', an 8-way data output 22 to a splitter cable 'SKT' and a control signal input 24 from an interface card 'I/O Card'.

With no voltage applied to any of the relays 'Rly 1' to

'Rly 4', inputs 1,2,3 and 6 from 'PC' are routed to the corresponding outputs of 'SKT' as shown in Figure 4A. However, the circuit is re-configurable by applying an appropriate pattern of control signals to 'I/O Card'. These signals are amplified by IC1, a 'Darlington driver' circuit, in order to produce corresponding output voltages capable of switching one or more of the relays 'Rly 1' to 'Rly 4', thereby re-routing certain of the 'PC' input data signals to alternative 'SKT' outputs.

Figure 4B illustrates the effect of applying an 'ALL 1's' signal to inputs 4 to 7 of 'I/O Card', thereby switching all four relays so that inputs 1,2,3 and 6 of 'SKT' are re-routed to outputs 4,5,7 and 8 of 'SKT' respectively.

Inputs 1 and 2 of 'I/O Card' connect a supply voltage and a ground respectively. A signal applied to input 3 of 'I/O Card' will turn on light-emitting-diode Led1 which may be used to indicate the current state of the device.

In the example of Figure 4, outputs 1,2,3 and 6 of 'SKT' are connected via a splitter cable to the corresponding data lines of a local network bus, while outputs 4,5,7 and 8 are connected to a remote network e.g. the Internet.

It will be appreciated that the arrangement shown in Figure 2 can be achieved by reconfiguring the arrangement shown in Figure 1, that is to say the existing cable can be used, and no new cable installation is needed.

Claims

1) A computer system comprising two or more independent data networks and at least one computer terminal, the or each computer terminal having a switching means associated therewith for selectively interfacing that computer terminal with any one of said data networks, one-at-a-time, via respective communication channels.

2) A computer system as claimed in Claim 1, wherein one of said data networks comprises an external network.

3) A computer system as claimed in Claim 1 or 2, wherein the or each said switching means is incorporated into its respective computer terminal.

4) A computer system as claimed in Claim 1 or 2, wherein the or each said switching means comprises a separate unit connected to its respective computer terminal.

5) A computer system as claimed in any preceding claim, wherein the or each said computer terminal comprises a personal computer (PC).

6) A computer system as claimed in any preceding claim, wherein the or each said switching means comprises a plurality of data routing circuits which are electrically or electronically re-configurable according to control signals issued by its respective computer terminal.

7) A computer system as claimed in Claim 6, wherein said electronically re-configurable data routing circuits comprise electromagnetic relay devices driven by Darlington amplifier circuits.

8) A computer system as claimed in any preceding claim, wherein the or each said switching means receives data and/or control signals either directly via the internal bus system of its respective computer terminal, or indirectly via a parallel

or serial interface card.

9) A computer system as claimed in any preceding claim, wherein the or each said switching means is controlled via software driver routines running on its respective computer terminal.

10) A computer system as claimed in any preceding claim, wherein the or each said switching means routes data via one or other of two 4-way data channels comprising an 8-way 'splitter' cable.

11) A computer system as claimed in any preceding claim, wherein network data is carried by an unshielded twisted pair cable.

12) A computer system as claimed in any of claims 1 to 10, wherein network data is carried by a shielded coaxial cable.

13) A computer system as claimed in any of claims 1 to 10, wherein network data is carried by a fibre-optic cable.

14) A computer input/output interface card, comprising parallel and/or serial interface circuitry, and switching means for selectively interfacing said interface circuitry with any one of a plurality of independent computer data networks, one-at-a-time, vie respective communication channels.

15) A switching device for selectively interfacing a computer with any one of a plurality of independent data networks, one-at-a-time, via respective communication channels.

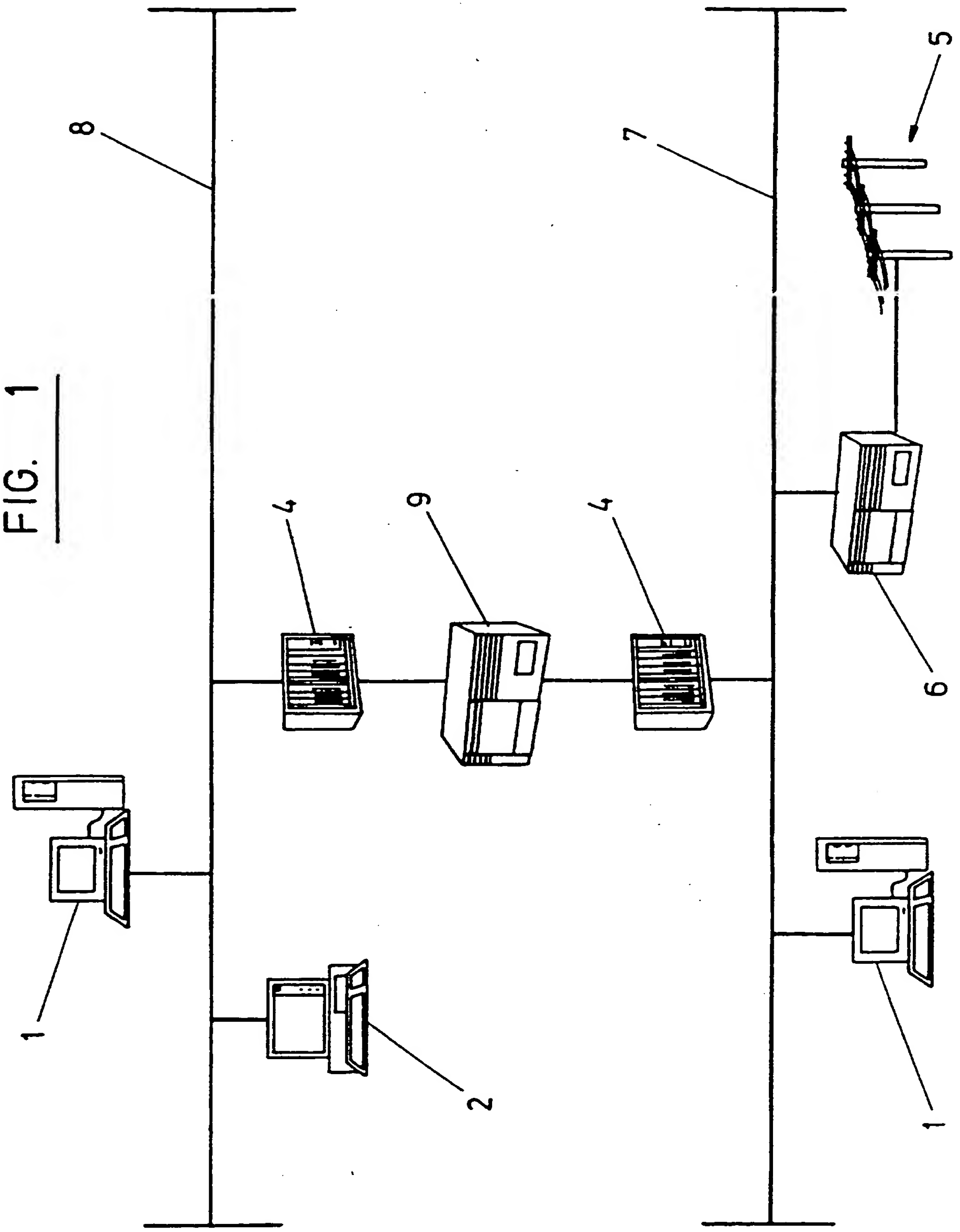


FIG. 1

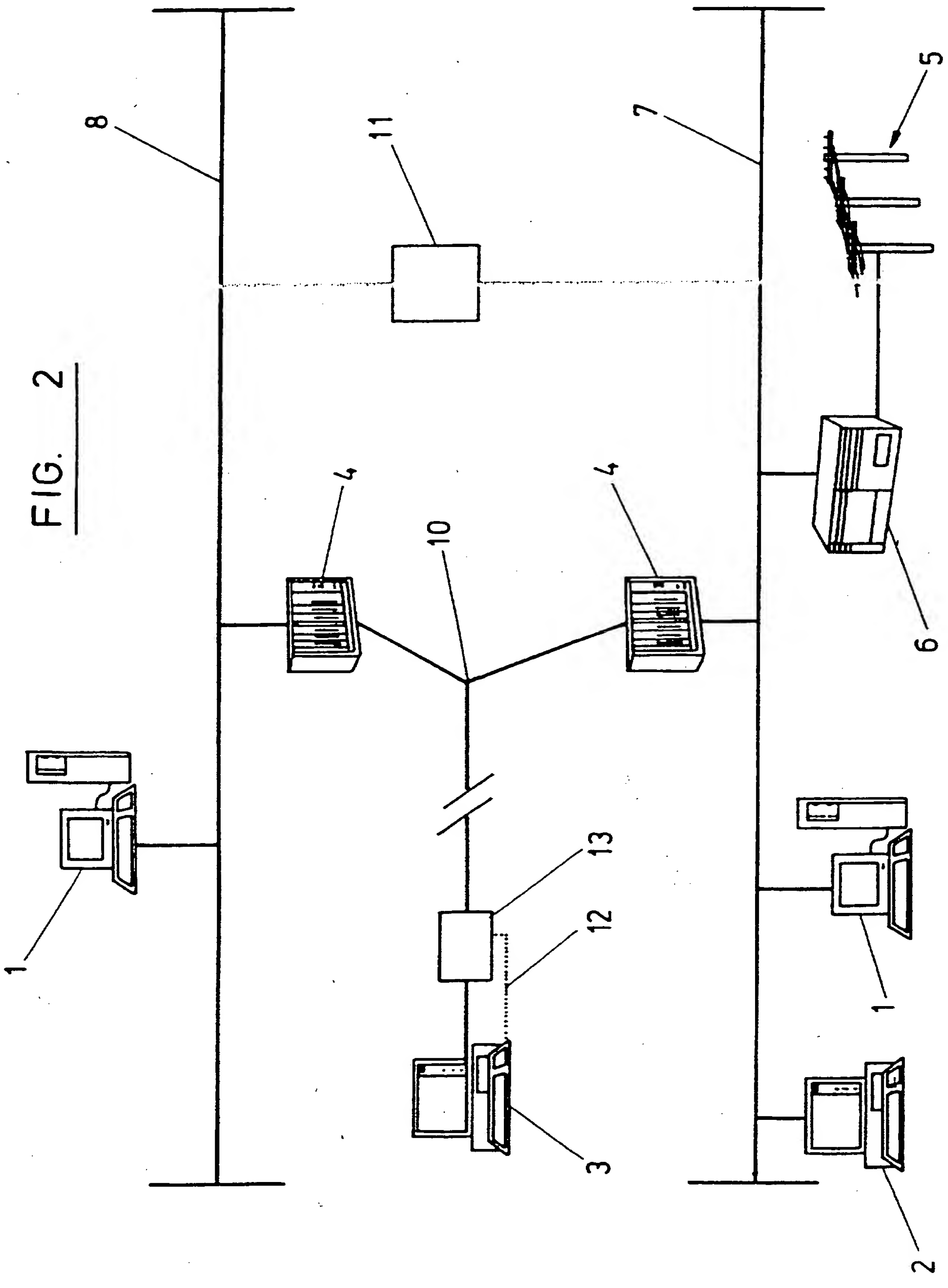


FIG. 2

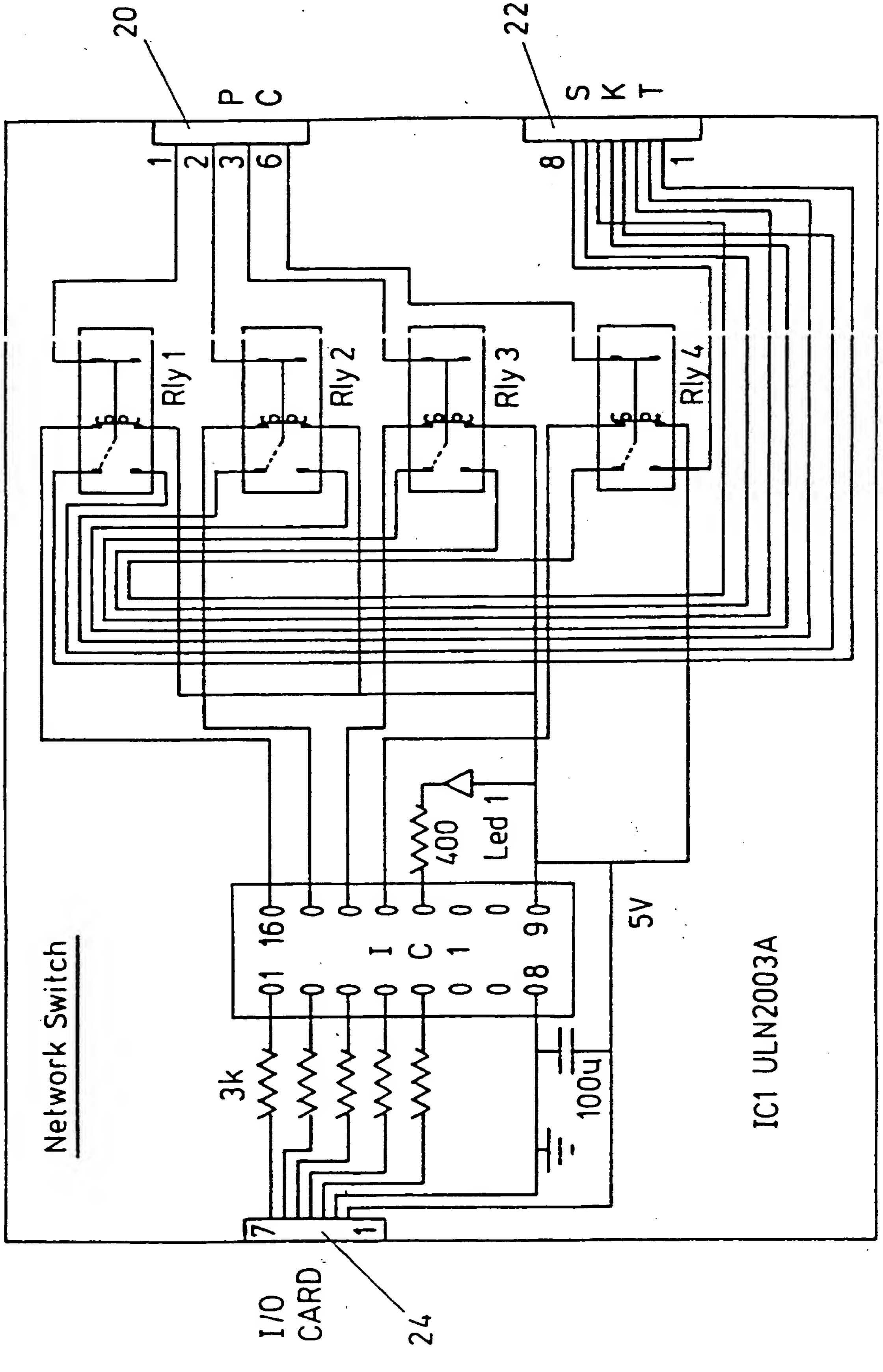

20
22
PC
SKT
1
2
3
6
8
1
Rly 1
Rly 2
Rly 3
Rly 4
Network Switch
400
Led 1
16
9
1
8
IC1
5V
3k
100u
IC1 ULN2003A
7
1
I/O CARD
24

FIG. 3

Network Switch PC to SKT assignments.

- Local network connection

PC socket (pin)	SKT socket (pin)
1	1
2	2
3	3
6	6

- Remote network connection (e.g. Internet)

PC socket (pin)	SKT socket (pin)
1	4
2	5
3	7
6	8

FIG. 4

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/22, 12/46, 29/06

A3

(11) International Publication Number: WO 97/16782

(43) International Publication Date: 9 May 1997 (09.05.97)

(21) International Application Number: PCT/GB96/02561

(22) International Filing Date: 17 October 1996 (17.10.96)

(30) Priority Data:

9521407.8	18 October 1995 (18.10.95)	GB
9602615.8	9 February 1996 (09.02.96)	GB

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

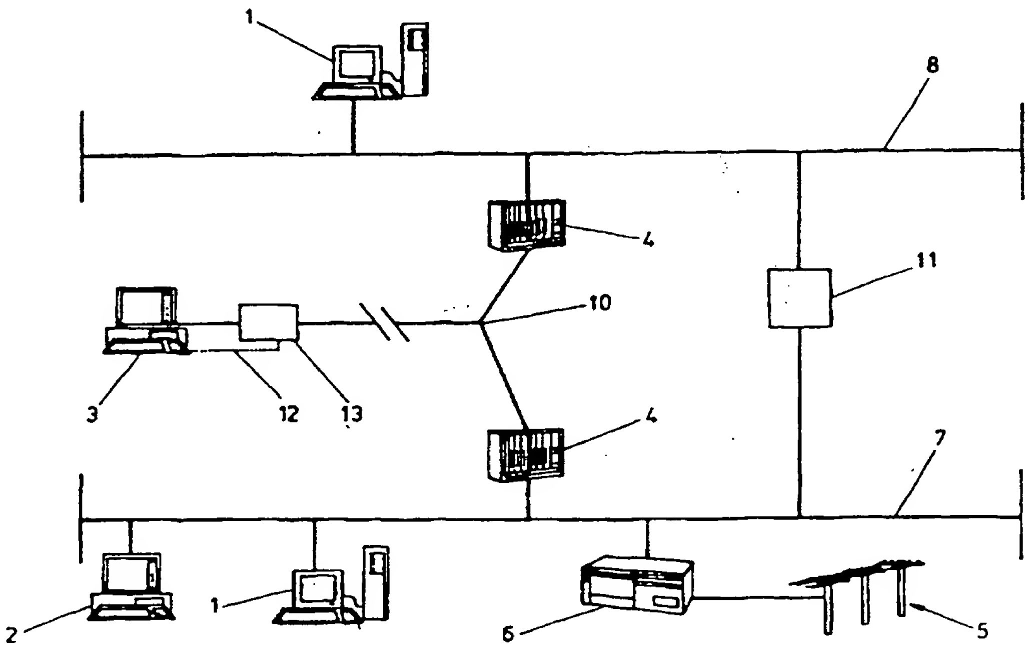
(71)(72) Applicant and Inventor: HOLBOROW, Leslie, Christopher [GB/GB]; 10 Mydam Lane, Gorseinon, Nr. Swansea, West Glamorgan SA4 4YA (GB).

(74) Agent: GIBSON, Stewart, Harry; Urquhart-Dykes & Lord, Three Trinity Court, 21-27 Newport Road, Cardiff CF2 1AA (GB).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report:
26 June 1997 (26.06.97)

(54) Title: COMPUTER NETWORK SECURITY ARRANGEMENTS



(57) Abstract

A computer system comprises two or more independent data networks (7, 8) and at least one computer terminal (3). The or each computer terminal has a switching means (13) associated with it, for selectively interfacing that terminal with any one of the data networks, one-at-a-time, via respective communication channels.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 96/02561

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/22 H04L12/46 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 153 567 A (SINCLAIR RESEARCH LIMITED) 21 August 1985 see page 1, left-hand column, line 6 - right-hand column, line 129 see figure 1	1-3,5-15
A		4

X	GB 2 283 154 A (QUEST STANDARD TELEMATIQUE S.A.) 26 April 1995 see page 1, line 3 - page 2, line 24 see page 5, line 19 - page 8, line 1 see figures 1,2	1,2,4-8, 10-13,15
A		3,9,14

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search 29 April 1997	Date of mailing of the international search report 16.05.97
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Authorized officer Vaskimo, K

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 96/02561

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 91 18462 A (THE UNIVERSITY OF TORONTO INNOVATIONS FOUNDATION) 28 November 1991 see page 3, line 31 - page 4, line 22 see page 5, line 11 - line 18 see page 6, line 20 - page 7, line 26 see page 13, line 4 - page 14, line 24 see figures 1,4	1,4-6, 11-13,15
A		2,3, 7-10,14

A	US 5 444 856 A (BOWERS ET AL.) 22 August 1995 see column 1, line 6 - line 10 see column 3, line 14 - column 4, line 3 see column 4, line 39 - line 53	1,2,4-6, 11-13,15

A	EP 0 350 674 A (BULL HN INFORMATION SYSTEMS INC.) 17 January 1990 see column 1, line 48 - column 2, line 39 see column 4, line 27 - line 41 see column 5, line 29 - line 47 see figures 1,2	1,4-7, 14,15

A	US 4 555 593 A (O'DEA) 26 November 1985 see column 1, line 5 - line 13 see column 7, line 53 - column 8, line 2 see figure 4	1,7

A	SARGENT M., SHOEMAKER R.L.: "The IBM Personal Computer From the Inside Out" 1994 , ADDISON WESLEY , US XP002030448 020317 see page 355 - page 397	1,8

A	EP 0 508 886 A (DIGITAL EQUIPMENT CORPORATION) 14 October 1992 see column 1, line 3 - column 2, line 35 see figures 1,5	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/GB 96/02561

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2153567 A	21-08-85	NONE	
GB 2283154 A	26-04-95	FR 2711468 A	28-04-95
WO 9118462 A	28-11-91	NONE	
US 5444856 A	22-08-95	NONE	
EP 350674 A	17-01-90	US 4999787 A AU 617491 B AU 3801089 A	12-03-91 28-11-91 18-01-90
US 4555593 A	26-11-85	NONE	
EP 508886 A	14-10-92	DE 69217103 D JP 5114905 A US 5515513 A	13-03-97 07-05-93 07-05-96